DEPARTMENT OF THE ARMY
HEADQUARTERS, 2ND INFANTRY DIVISION
UNIT #15041
APO AP 96258-5041

REPLY TO
ATTENTION OF:

EAID-CG

18 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter # 13, Information Assurance

1. This policy is effective immediately and remains in effect until rescinded or superseded.

2. References:

a. DoD 5200.1R, Information Security Program, 14 January 1997.

b. DoD 8500.1, Information Assurance, 24 October 2002.

c. DoDI 8500.2, Information Assurance Implementation, 6 February 2003.

d. USFK Command Policy Letter #13, Information Assurance, 26 June 2006.

3. This policy applies to all members of the 2ID when in the territory of the Republic of Korea, which includes personnel on PCS, TDY, pass or leave status, DoD civilians, DoD-invited contractors/technical representatives, and their respective family members and visiting guests.

4. Subordinate commanders must ensure that our information systems are protected and defended against exploitation, denial of service, and unauthorized access. This policy is designed to provide general guidance on Information Assurance (IA) managing removable media (USB/Thumb Drives, CDs, DVDs, Diskettes, etc.), and managing unclassified e-mails.

5. All personnel are charged with adhering to the specific policy guidance below.

a. General Information Assurance.

(1) Protect Information: All personnel will safeguard data within the computing environment and ensure all data is appropriately labeled, handled, stored, transported, and disposed of IAW ref 2a. Personnel and organizations will immediately notify their technical chain and Information Assurance support channels when irregular computer activity is suspected.

(2) Defend Systems and Networks: Everyone must recognize, react and respond to threats, vulnerabilities, and deficiencies. Information Systems Service Providers will ensure that access is controlled, and all systems/networks incorporate defense-in-depth strategies and tools.

(3) Create an IA-Empowered Workforce: Subordinate commanders will ensure that all users receive Information Assurance training before they are granted access to government information systems.

b. Removable Storage Media (USB/Thumb Drives, CDs, DVDs, Diskettes, etc.). All personnel must mitigate the risk of compromising classified information stored on removable storage media. These media have multiple uses and their small size and adaptability can result in loss of accountability and inappropriate cross net (SIPR to NIPR, etc.) use. Recent revelations of this loss of accountability outside the gate in Baghram, Afghanistan highlight the requirement for focused command oversight. Commanders and Designated Approval Authorities will allow the specific use of removable media on an exception only basis, and institute rigid control mechanisms for accounting, handling, labeling, transporting and disposing of this classified media.

c. Unclassified e-mail. All personnel must have the capability to digitally sign and encrypt official e-mail containing sensitive and/or critical information, or other information that could potentially be exploited by unfriendly enterprises or an adversary. A good rule of thumb is that unless you want to read it in the public media, you need to encrypt it. Unclassified information which should be encrypted on our NIPRNET may include:

(1) Information under the Privacy Act, and the Health Insurance Portability and Accountability Act of 1996.

(2) Information for Official Use Only (FOUO).

(3) Unclassified unit status, capabilities, vulnerabilities (i.e., facilities, information systems, force protection).

(4) Travel itineraries for key leadership personnel.

(5) User names/passwords.

(6) Information found in routine DoD payroll, finance, logistics, and personnel management systems.

(7) All e-mail sent to and from the Commanding General, 2nd Infantry Division will be digitally signed and encrypted. Encrypted e-mails received from the Commander will not be forwarded to anyone unencrypted.

6. Questions regarding this policy should be directed to the 2ID Information Assurance Office, DSN 732-6571.

James A. Coggin
JAMES A. COGGIN
Major General, USA
Commanding

DISTRIBUTION:
A